

CENTRAL FAX CENTER

JAN 29 2007

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

REMARKS

This amendment is responsive to the Final Office Action dated November 27, 2006. Applicant has amended claims 1, 2, 3, 6, 7, 13, 22, 26, and 27, and cancelled claims 5 and 25. Claims 1-4, 6-24, 26-55 remain pending, with claims 16-18 and 36-55 currently being withdrawn due to restriction.

Claim Amendments

Applicants have amended claim 1 to clarify that the authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern, wherein the access control attribute is a coarse-grain access control attribute defining access control rights for resources provided by a device. These elements were previously recited in Applicant's claim 5, now cancelled. Consequently, no new issues have been raised and this amendment should be entered.

Applicants have amended claim 1 to clarify that the "command" is received from a client and that the command requests access to configuration data of the device. Pending claim 7, now amended, previously recited that the command was received from a client; therefore, this amendment should raise no new issues. Applicant respectfully requests that the amendment be entered.

Applicants have also amended claim 1 to recite that controlling access to the configuration data by the client based on the coarse-grain access control attribute and the evaluation of the regular expression. Claim 5, now cancelled, previously recited controlling access to the configuration data based on the coarse-grain access control attribute and the evaluation of the regular expression. Consequently, no new issues have been raised and this amendment should be entered.

Similar amendments have been made to independent claim 22.

Claim Rejection Under 35 U.S.C. § 102

In the Final Office Action, the Examiner rejected claims 1-3, 15, 22-24, and 35 under 35 U.S.C. 102(b) as being anticipated by Valois (US 2004/0260818). Valois fails to disclose each

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

and every feature of the claimed invention, as required by 35 U.S.C. 102(e), and provides no teaching that would have suggested the desirability of modification to include such features.

Valois

Valois describes a system and method for testing the security policies of a network device, and verifying that the device implements its intended security policy.¹ In particular, Valois describes a software system that is a “*tool in diagnosing the security vulnerability of a network device.*”² FIG. 1 of Valois shows that the software tool verifies that a device or a plurality of devices correctly implements their intended security policies.³ The software tool of Valois includes a configuration repository database 12, a security policy database 14, a test scripts database 16, a validation engine 18, and a parser engine 20. According to Valois, the test scripts database of the software testing system contains a collection of test scripts or expert rules that expresses a security characteristic or policy for testing the different network devices.⁴ Valois describes that these test scripts of the verification software system may utilize regular expressions to search configuration files of the network devices to verify compliance with the desired security policies.⁵

In contrast, the present application describes in detail a device, such as a router, that supports a set of access control attributes, e.g., permissions bits, that provide course-grain access control over groups of resources. In addition, regular expressions may also be specified in conjunction with the access control attributes to provide fine-grain access control to the resources. If the regular expressions are defined, the device applies the regular expressions associated with the fine-grain access control class attributes to evaluate text-based commands provided by the clients and selectively allow or deny access requests to access configuration data within the device based on the evaluation. See, e.g., paragraph [0008].

Claim 1 is directed to a method comprising storing authorization data that defines an access control attribute and an associated regular expression defining a textual pattern, wherein

¹ Valois at Summary.

² Valois at 0068 (emphasis added).

³ Valois at 0049.

⁴ Valois at 0055.

⁵ Valois at 0057, 0058.

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

the access control attribute is a coarse-grain access control attribute defining access control rights for resources provided by a device. Amended claim 1 specifically requires receiving the command from a client, wherein the command requests access to configuration data of the device. Claim 1 further requires evaluating the command using the regular expression to determine whether the command matches the textual pattern, and controlling access to configuration data of a device by the client based on the coarse-grain access control attribute and the evaluation of the regular expression. Applicant submits that the Valois software system for verifying network devices fails to teach or suggest nearly every one of these features.

With respect to the present claims, the Examiner asserted that the Valois reference teaches evaluating a command using a regular expression to determine whether the command matches the textual pattern. Specifically, the Examiner reasoned that the Valois network verification tool evaluates Access Control Lists (ACLs) that can be viewed as "commands" that specify whether resources can be accessed or denied. Final Office Action, pg. 12.

The current amendments render this argument moot. Specifically, Applicant's claims 1 and 22 clearly require that the command be received from a client and the command request access to configuration data. That is, consistent with Applicant's specification and claims, a client command to access configuration data is evaluated using the specified regular expression associated with the access control attribute. The Valois validation tool uses regular expressions to verify that configuration data refers to defined access control lists. This is entirely different from Applicant's claims that require receiving a command from a client, wherein the command requests access to the configuration data. It should be clear from the plain language of claim 1 that the "command" being validated is a request to access configuration data, and not an ACL or other access control attribute.

The Examiner also asserted that the Valois reference teaches controlling access to configuration data based on the evaluation of the regular expression. Specifically, the Examiner reasoned that the Valois network verification tool "controls access to configuration data" merely because it extracts references from the configuration repository database and performs a comparison matching. The Examiner stated that the process of extracting and comparing configuration data corresponds to the act of controlling access to configuration data. Final Office Action, pg. 13. In other words, to the best of Applicants' understanding, the Examiner asserts

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

that execution of the Valois tool to interrogate the configuration repository is a form of "controlling access to the configuration repository" in that the execution flow of the Valois tool impacts how the repository is accessed by the tool itself.

The current amendments render this argument moot as well. Specifically, Applicants' claims 1 and 22 require *controlling access to the configuration data by the client* based on the coarse-grain access control attribute and the evaluation of the regular expression. That is, it is access to the configuration data by the client that is being controlled based on both the coarse-grain access control attribute and the evaluation of the regular expression to the command received from the client. This is entirely different from simply interrogating configuration data with an ACL validation tool, as described by Valois.

For at least these reasons, Valois fails to establish a prima facie case for anticipation of Applicant's claims under 35 U.S.C. 102(b). Withdrawal of this rejection is requested.

Claim Rejection Under 35 U.S.C. § 103

The Examiner rejected claim 19 and its dependent claims under 35 U.S.C. 103(a) as being unpatentable over Valois (USPN 2004/0260818) in view of Delany (USPN 2002/0156879) and further in view of Nelson (USPN 6,243,713).

Claim 19 requires receiving input defining an access control attribute and an associated regular expression that specifies a textual pattern, and pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression. Claim 19 literally requires evaluating a command in real-time using the regular expression as a client enters the command via a command line interface, and controlling access to configuration data of a device based on the evaluation.

With respect to the rejection of claim 19, the Examiner stated that "Valois was relied upon within prior claims to disclose the limitation of the evaluation of commands." Final Office Action, pg. 16. As discussed above, the Examiner asserted that Valois teaches evaluating a command using a regular expression since the Valois network verification tool evaluates lists of rules, i.e., Access Control Lists (ACLs). The Examiner asserted that the ACLs evaluated by the Valois tools are "commands" that specify whether resources can be accessed or denied. Final Office Action, pg. 12.

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

Therefore, it is the Examiner's position that one of ordinary skill would modify the Valois validation tool in view of Delany and Nelson so that it evaluates an ACL in real-time as a client enters the ACL via a command line interface, thereby teaching or suggesting Applicants' claim 19. Applicant submits that this logic breaks down with respect to the literal language of claim 19.

For example, the literal language of claim 19 differentiates between an access control attribute and a command entered by a client. That is, claim 19 separately requires an access control attribute, a regular expression associated with the access control attribute, and a command received from a client. The Examiner cannot argue that the access control lists in Valois is an access control attribute having associated regular expression and then at the same time argue that it is a command evaluated using the regular expression as the client enters the command. These are separate elements with claim 19.

Moreover, the literal language of claim 19 requires separate steps for receiving input that defines the access control attribute and an associated regular expression, and evaluating a command with the regular expression as the client enters the command. This further makes clear that the access control attribute and the command must be entered separately, and that the command simply cannot be the same element as the access control attribute.

The Examiner's position that the ACLs in Valois are "commands" that are evaluated by the Valois tool using a regular expression, ignores the separate requirements of claim 19 that (1) input is received defining both the access control attribute and the regular expression, and (2) that the regular expression is pre-processed to evaluate a command as the command is entered. If the ACLs evaluated by the Valois tool are to be considered commands, then it would be impossible for Valois to meet the requirement of receiving input defining the access control attribute and the regular expression separately from evaluating a command as the command is entered.

Applicant's can see no teaching within the cited references as to how the Valois validation tool can be modified to use input defining an access control attribute and an associated regular expression to evaluate a command in real-time as a client enters the command. For at least these reasons, the cited references fail to establish a prima facie case for non-patentability of Applicant's claims under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

RECEIVED
CENTRAL FAX CENTER

JAN 29 2007

Application Number 10/628,885
Amendment dated January 29, 2007
Responsive to Office Action mailed November 27, 2006

CONCLUSION

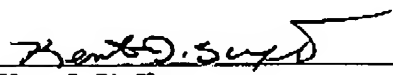
All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

By:

January 29, 2007

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102


Name: Kent J. Sieffert
Reg. No.: 41,312